YSOFT SAFEQ Cloud®

WEBINAR

WEBINAR Q&A SESSION – A WORLD WITH MODERN AUTHENTICATION

Question 1: Why isn't modern authentication used for the messaging function?
Answer: Modern authentication is currently being implemented for messaging services and is currently scheduled for release by the end of October.

Question 2: Can you support Phone Logins like OpenPath Vigilon?
Answer: At this moment we do not support any such specific systems. With future development, we will depend on the demand from the market. Preferably, we would look at OpenID and then potentially FIDO is the direction that that we want to take.

Question 3: Are there any plans for paragon cloud to support GCC for US Government?
Answer: That is a very complex topic, because supporting the Federal and State government in in the USA is not just about card supports but adhering to many more regulations. We are looking into a business case on supporting the US Government as bulk. But at this moment this is still on the business evaluation side.

Question 4: Will guest accounts be able to sign up via simple buttons? (Google, Apple, Microsoft etc.)
Answer: We had a lot of discussion about wanting to have this support. Potentially, the back end can support it, but we did not register enough need for implementing it. If we see there is a demand and it is aligned with our principal direction of development, then we will consider it.

Question 5: Manual Login to SQ Cloud is being deprecated in SQ CLOUD CLIENT – I believe it is a very important feature for small installations at customers without identity provider. We used to have a customer some time ago with 100 PCs and all usernames were USER1, so we had to use SQ Client. If this option is deprecated such installation will be impossible.
Answer: Manual login is still possible, and it still will be possible. The only difference that instead of seeing little pop-up with the username and password as a little window, you will see a larger window showing our unified authentication screen. And you can still type in your local username and local password from the application.

On the on the back end we are acting as the OpenID connect or IDC provider towards the client. And even though technically on the back end, we still have the password hash somewhere in our cache. There is a token-based communication to the customer.

Question 6: Microsoft doesn't recommend using service accounts. Do you support user principal names?
Answer: Not at this moment. The key difference is that's the usernames that we have at this moment in the service accounts can change. And that's the reason of the recommendation. I don't believe that there is strict security reason per se. Even though, changing the name is potential security flaw. We will be implementing and will be adding it in upcoming releases to upcoming updates. And the support for the user principles as well.

Question 7: With all of the changes/enhancements, when configuring an Entra ID Auth profile, is it still necessary to configure a Conditional Access policy in Entra ID when MFA is enabled?
Answer: There is no CA policy needed.